USE CASE

TOOL CONSOLIDATION

A holistic approach ensures continuous security across the supply chain

BACKGROUND

Recent security events such as Log4j, Solarwinds, and Equifax have highlighted just how vulnerable software supply chains are to attacks from malicious actors. In 2022 alone there were over 26,000 new CVEs reported. Most CVEs are unintentional vulnerabilities in popular packages and libraries, but the JFrog Security Research team discovered 1460 new intentionally malicious packages in the same time span.

Organizations are moving aggressively to ensure the integrity of their software supply chains. Between SAST, DAST, SCA and the multiple other types of application security solutions it's possible for organizations to have a dozen different tools in place to ensure their released software applications are free from exploitable vulnerabilities.

More point solutions however, don't guarantee a comprehensive approach to application security. A glut of security tools creates its own issues including integration overhead and missing blindspots, a flood of security issues to track across different tools, prioritization and remediation overhead, and increased manual security efforts.

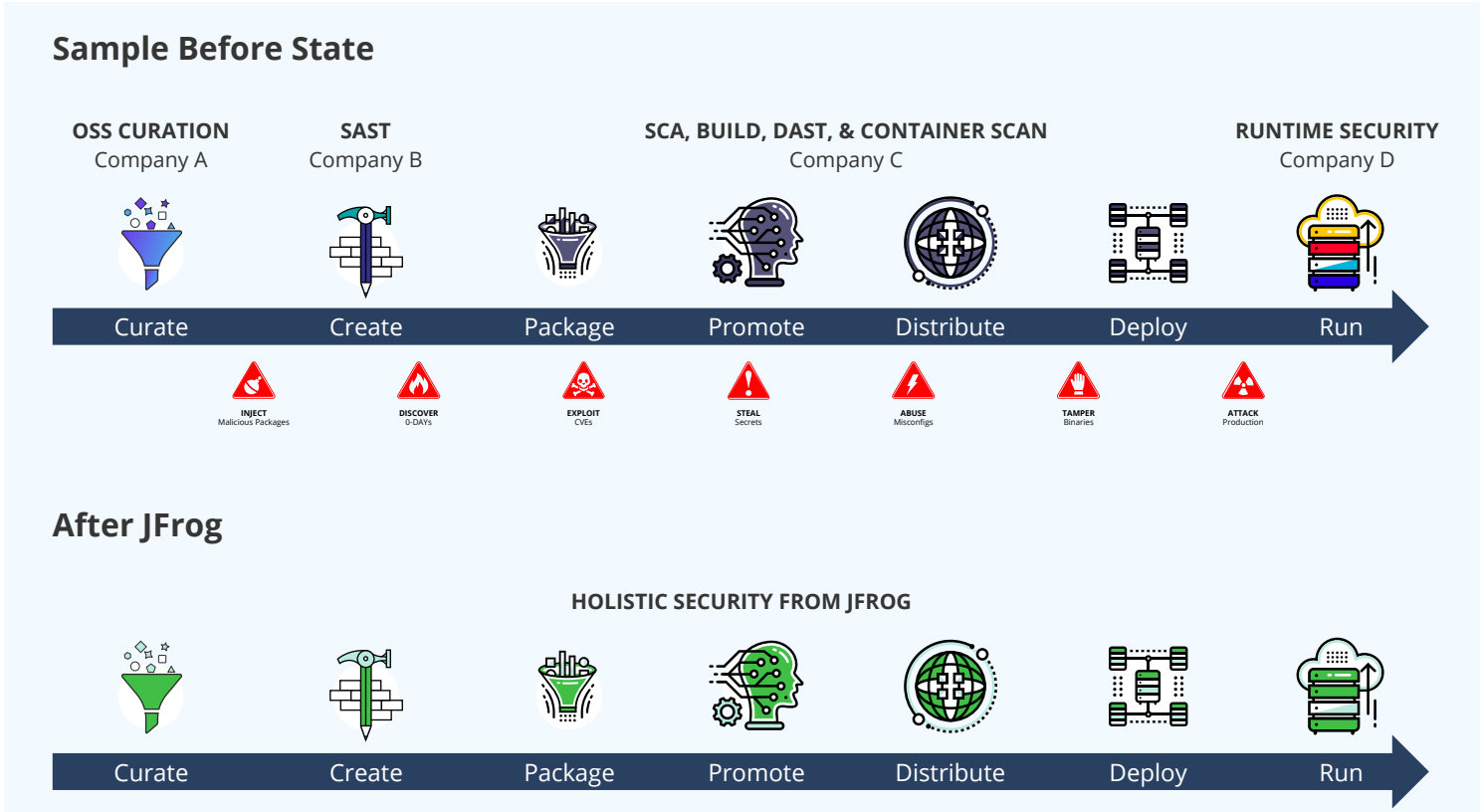
These issues negatively impact developer velocity and security risk. Ultimately, Security and DevOps teams are forced to try and apply policies consistently using multiple applications without a single pane of glass into the overall security of their component ecosystem.

SOLUTION

JFrog eliminates the need for point security solutions in favor of a holistic binary focused approach, bolstered by a leading research team, that ensures continuous security across the supply chain. By shifting left security efforts and applying them continually and consistently throughout the software lifecycle, organizations can be confident that the software they're releasing is safe and secure.

Key capabilities supporting security tool consolidation with JFrog:

- Enhanced SCA, Malicious Package Detection, IaC Security, Secrets Detection, Services and Application Exposures Detection
- Shift left security with IDE plugins, CLI Tool, Docker Desktop extension and a Git repository scanner
- Contextualized analysis to prioritize vulnerabilities with developer friendly remediation instructions
- Automated SBOM creation (and export) in SPDX, CycloneDX standard formats
- Support for the leading OSS package and technology types (and growing)
- Policies to fail builds, block promotion, and trigger workflows
- Policies to curate an approved set of packages for developers to use
- Application security as a native part of the JFrog platform that integrates with popular CI/CD and DevOps tools
- Signed pipelines and builds



By focusing on five core tenets — Developer Focus, Efficiency, Accuracy, Coverage, and Prioritization — JFrog can deliver unbeatable protection from all potential supply chain threats whether self-hosting or making use of public clouds.

RESULTS

Fast Remediation

Find and fix issues fast. JFrog customers resolved Log4j issues in hours and days, not weeks and months

Cost Savings

Upwards of hundreds of thousands of dollars across license, maintenance, and integration costs

Proactive Prevention

Automated policies block vulnerabilities and malicious packages before they enter your ecosystem

Security Consistency

Ensure security policies and processes are applied consistently across all teams, projects, and developers

> *Something that's going to scan everything in that central repository of truth, automatically, with zero customization required, that's really, really powerful."*
>
> Larry Grill, DevSecOps senior manager, Hitachi Vantara

v1.0230501

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.

Start for free at https://jfrog.com/register/

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd